

TECHNOLOGY RESOURCES

CQ
(LOCAL)

Note: For Board member use of District technology resources, see BBI. For student use of personal electronic devices, see FNCE.

For purposes of this policy, "technology resources" means electronic communication systems and electronic equipment.

AVAILABILITY OF
ACCESS

Access to the District's technology resources, including the Internet, shall be made available to students and employees primarily for instructional and administrative purposes and in accordance with administrative regulations.

LIMITED PERSONAL
USE

Limited personal use of the District's technology resources shall be permitted if the use:

1. Imposes no tangible cost on the District;
2. Does not unduly burden the District's technology resources;
3. Does not occur while an employee is assigned to other duties; and
4. Has no adverse effect on an employee's job performance or on a student's academic performance.

No software may be installed or downloaded on District computers without the approval of the Superintendent or designee.

USE BY MEMBERS
OF THE PUBLIC

Access to the District's technology resources, including the Internet, may be made available to members of the public, in accordance with administrative regulations. Such use shall be permitted so long as the use:

1. Imposes no measurable cost on the District;
2. Does not unduly burden the District's technology resources; and
3. Follows procedures outlined in policy and regulation.

ACCEPTABLE USE

The Superintendent or designee shall develop and implement administrative regulations, guidelines, and user agreements consistent with the purposes and mission of the District and with law and policy.

Access to the District's technology resources is a privilege, not a right. All users shall be required to acknowledge receipt and understanding of all administrative regulations governing use of the District's technology resources and shall agree to allow monitoring of their use and to comply with such regulations and guidelines. Noncompliance may result in suspension of access or termination

TECHNOLOGY RESOURCES

CQ
(LOCAL)

of privileges and other disciplinary action consistent with District policies. [See DH, FN series, FO series, and the Student Code of Conduct]

Student access to District technology resources is permitted unless the parent has denied permission on the Student/Parent Handbook Parent Acknowledgement Form and returned the form to the campus.

Violations of law may result in criminal prosecution as well as disciplinary action by the District.

TERMINATION /
REVOCATION OF
SYSTEM USER
ACCOUNT

Termination of an employee's or student's access for violation of District policies or regulations shall be effective on the date the principal or chief technology officer receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

INTERNET SAFETY

The Superintendent or designee shall develop and implement an Internet safety plan to:

1. Control students' access to inappropriate materials, as well as to materials that are harmful to minors;
2. Ensure student safety and security when using electronic communications;
3. Prevent unauthorized access, including hacking and other unlawful activities;
4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students; and
5. Educate students about cyberbullying awareness and response and about appropriate online behavior, including interacting with other individuals on social networking Web sites and in chat rooms.

FILTERING

Each District computer with Internet access and the District's network systems shall have filtering devices or software that blocks access to visual depictions that are obscene, pornographic, inappropriate for students, or harmful to minors, as defined by the federal Children's Internet Protection Act and as determined by the Superintendent or designee.

The Superintendent or designee shall enforce the use of such filtering devices. Upon approval from the Superintendent or designee, an authorized technology staff member may disable the filtering device for bona fide research or other lawful purpose.

TECHNOLOGY RESOURCES

CQ
(LOCAL)

MONITORED USE	Electronic mail transmissions and other use of the District's technology resources by students, employees, and members of the public shall not be considered private. Designated District staff shall be authorized to monitor the District's technology resources at any time to ensure appropriate use.
DISCLAIMER OF LIABILITY	The District shall not be liable for users' inappropriate use of the District's technology resources, violations of copyright restrictions or other laws, users' mistakes or negligence, and costs incurred by users. The District shall not be responsible for ensuring the availability of the District's technology resources or the accuracy, age appropriateness, or usability of any information found on the Internet.
RECORD RETENTION	A District employee shall retain electronic records, whether created or maintained using the District's technology resources or using personal technology resources, in accordance with the District's record management program. [See CPC]
SECURITY BREACH NOTIFICATION	<p>Upon discovering or receiving notification of a breach of system security, the District shall disclose the breach to affected persons or entities in accordance with the time frames established by law.</p> <p>The District shall give notice by using one or more of the following methods:</p> <ol style="list-style-type: none">1. Written notice.2. Electronic mail, if the District has electronic mail addresses for the affected persons.3. Conspicuous posting on the District's Web site.4. Publication through broadcast media.